

(e) *Inspection, testing, and maintenance.* Each railroad shall develop and adopt written procedures for the inspection, testing, and maintenance of all fire safety systems and fire safety equipment on the passenger equipment it operates. The railroad shall comply with those procedures that it designates as mandatory for the safety of the equipment and its occupants.

[64 FR 25660, May 12, 1999, as amended at 67 FR 42909, June 25, 2002]

#### § 238.105 Train electronic hardware and software safety.

The requirements of this section apply to electronic hardware and software used to control or monitor safety functions in passenger equipment ordered on or after September 8, 2000, and such components implemented or materially modified in new or existing passenger equipment on or after September 9, 2002.

(a) The railroad shall develop and maintain a written hardware and software safety program to guide the design, development, testing, integration, and verification of software and hardware that controls or monitors equipment safety functions.

(b) The hardware and software safety program shall be based on a formal safety methodology that includes a Failure Modes, Effects, Criticality Analysis (FMECA); verification and validation testing for all hardware and software components and their interfaces; and comprehensive hardware and software integration testing to ensure that the hardware and software system functions as intended.

(c) The hardware and software safety program shall include a description of how the following will be accomplished, achieved, carried out, or implemented to ensure safety and reliability:

- (1) The hardware and software design process;
- (2) The hardware and software design documentation;
- (3) The hardware and software hazard analysis;
- (4) Hardware and software safety reviews;
- (5) Hardware and software hazard monitoring and tracking;

(6) Hardware and software integration safety testing; and

(7) Demonstration of overall hardware and software system safety as part of the pre-revenue service testing of the equipment.

(d) (1) Hardware and software that controls or monitors a train's primary braking system shall either:

(i) Fail safely by initiating a full service brake application in the event of a hardware or software failure that could impair the ability of the engineer to apply or release the brakes; or

(ii) Access to direct manual control of the primary braking system (both service and emergency braking) shall be provided to the engineer.

(2) Hardware and software that controls or monitors the ability to shut down a train's main power and fuel intake system shall either:

(i) Fail safely by shutting down the main power and cutting off the intake of fuel in the event of a hardware or software failure that could impair the ability of the train crew to command that electronic function; or

(ii) The ability to shut down the main power and fuel intake by non-electronic means shall be provided to the train crew.

(e) The railroad shall comply with the elements of its hardware and software safety program that affect the safety of the passenger equipment.

[67 FR 19990, Apr. 23, 2002]

#### § 238.107 Inspection, testing, and maintenance plan.

(a) *General.* Beginning on January 1, 2002, the following provisions of this section apply to railroads operating Tier I passenger equipment covered by this part. A railroad may request earlier application of these requirements upon written notification to FRA's Associate Administrator for Safety as provided in § 238.1(c).

(b) Each railroad shall develop, and provide to FRA upon request, a detailed inspection, testing, and maintenance plan consistent with the requirements of this part. This plan shall include a detailed description of the following:

- (1) Inspection procedures, intervals, and criteria;
- (2) Test procedures and intervals;